

Salina man charged with raping 13-year-old girl

Print Email



By Jacob Pucci | jpucci@syracuse.com

Email the author | Follow on Twitter

on October 02, 2015 at 2:21 PM, updated October 02, 2015 at 2:32 PM



William Raymond Onondaga County Sheriff's Office

SALINA, N.Y. -- A 35-year-old Salina man was arrested on charges that he twice raped a 13-year-old girl.

William B. Raymond III, of [REDACTED], faces two counts each of second-degree rape, second-degree criminal sex act and endangering the welfare of a child, Onondaga County Sheriff's Detective Jon Seeber said.

Deputies were alerted after the girl told a family member about her relationship with Raymond, Seeber said.

Raymond was arrested on Sept. 24 and arraigned in Salina Town Court. Due to Raymond having two or more felony convictions, he was ordered held without bail at the Onondaga County Justice Center.

In 2000, Raymond was convicted of felony grand larceny and in 2012, was arrested for failing to pay restitution in connection with the conviction.

ADVERTISING

inRead invented by Teads

Contact Jacob Pucci: Email | Twitter | 315-766-6747



United States Department of Justice

*United States Attorney
Northern District of New York*

100 South Clinton Street, P.O. Box 7198
James M. Hanley Federal Building
Syracuse, New York 13261-7198

Tel.: (315) 448-0672
Fax: (315) 448-0658

July 28, 2016

Randi Juda Bianco
Assistant Federal Public Defender
4 Clinton Square
Syracuse, New York 13202

Re: United States v. Clif Seaway

Dear Randi:

Pursuant to your request for additional early discovery, enclosed is a copy of the search warrant that authorized the search of your client's residence, together with the application and supporting documents.

Sincerely,

RICHARD S. HARTUNIAN
United States Attorney

A handwritten signature in black ink, which appears to read "Lisa M. Fletcher", is written over the typed name and title.

Lisa M. Fletcher
Assistant United States Attorney

Enclosures

SEARCH WARRANT

LOCAL CRIMINAL COURT, COUNTY OF OSWEGO, TOWN OF GRANBY, NY

TO ANY MEMBER OF THE NEW YORK STATE POLICE, U.S. DEPARTMENT OF HOMELAND SECURITY -
HOMELAND SECURITY INVESTIGATIONS, AND THE UNITED STATES MARSHAL SERVICE:

YOU ARE HEREBY DIRECTED TO SEARCH:

~~118 Germandale Dr., Patchen NY, 13669~~, and any other areas the residents may have custody or control of such as, but not limited to, the basement, the garage and other curtilage or vehicles on the property, including a light blue colored bus.

The residence is located on the north side of Germandale Dr., and is approximately ½ mile west of the intersection of County Road 8. The residence is a white colored mobile home with white skirting. There is a wooden front porch with a wooden railing located in front of the entrance door. The entrance door is white in color and there is dark trim along the roof line, and dark colored shutters on the windows. There is one shutter missing from a front window. To the right of the residence there is a light blue colored charter bus located on the property.

FOR THE FOLLOWING PROPERTY:

The property referred to and authorized to be seized, searched, held, and subsequently forensically examined is believed to contain evidence that will constitute, substantiate or support violations of Articles 130, 260, and 263 of the Penal Law of the State of New York, and this property is further described as follows:

1. Any and all computers, computer program, computer data and/or computer network information as those terms are defined in Penal Law 156.00.
2. Any computers, central processing units, external and internal drives, storage units or media, terminals and video display units, together with peripheral equipment such as keyboards, printers, modems, scanners, or digital cameras and their internal and external storage media.
3. Any and all computing or data processing software, or data including, but not limited to hard disks, floppy disks, magnetic tapes, and integral RAM or ROM units which may reveal evidence which substantiates violations of the aforementioned NY State Penal Law Statutes.
4. The following records and documents, whether contained or stored on the computer, cell phone, magnetic tape, cassette, CD disk, diskette, photo-optical device, Cloud Storage, or any other storage medium, in the form of Internet history, SMS, MMS, IM:
 - a. Any access numbers, passcodes, swipe code patterns, passwords, personal identification numbers (PINS), logs, notes, memoranda and correspondence relating to computer, electronic and voice mail systems, Internet addresses and/or related contacts.
 - b. Any computing or data processing literature, including, but not limited to printed copy, instruction books, notes, papers, or listed computer programs, in whole or in part.
 - c. Any audio or video cassette tape recordings, books, magazines, periodicals, or other recorded or printed material, the possession of which constitutes a violation of or supports a violation of Articles 130, 260, and/or 263 of the Penal Law of the State of New York.
 - d. Any and all photographs depicting sexual conduct by a child and/or minors engaged in sexually explicit conduct.
 - e. Records or correspondence relating to the possession, transmission, collection, trading, or production of the aforementioned photographs and/or videos.
5. Any internet capable device, such as cell phone, tablet, smartphone, gaming system that allows access to the Internet and allows for the transmission of data in violation of or supporting evidence of a violation of Articles 130, 260, 263 of the New York State Penal Law.

- You are directed to seize the same and, without unnecessary delay, return it to this court together with this warrant and a written inventory of such property subscribed and sworn to by you.
- You are directed to execute this warrant between the hours of 6:00am and 9:00pm.
- You are directed to forward seized property for forensic examination.
- You are authorized to convert it to humanly readable and viewable form as necessary.
- You are authorized, in the execution of this warrant, to enter the premises to be searched without giving notice of your authority or purpose.

This search warrant issued this 18th day of February 2016



(Hon. Donald E. Todd)

*County Court Judge sitting
as a local criminal court
pursuant to CPL 10.20(3)*

APPLICATION FOR SEARCH WARRANT
(Section 690.35 CPL)

STATE OF NEW YORK
COUNTY OF OSWEGO

LOCAL CRIMINAL COURT
TOWN OF GRANBY

To the Presiding Magistrate, Local Criminal Court, Town of Granby:

I, Inv. Michael R. Eckler, a Police Officer of the State of New York, to wit, an Investigator with the New York State Police, assigned locally to the Computer Crimes Unit – Northern Region, do hereby state that there is reasonable cause to believe that property of a kind or character described in Section 690.10 of the Criminal Procedure Law may be found in or upon a designated or described place, vehicle or person.

A. THE PROPERTY REFERRED TO AND SOUGHT TO BE SEIZED, SEARCHED, EXAMINED AND HELD (Sec 690.10 NYS CPL)

Constitutes evidence and tends to demonstrate that an offense was committed in this state, to wit, violations of Articles 130, 260, and 263 of the Penal Law of the State of New York; and

B. THE PROPERTY REFERRED TO AND SOUGHT TO BE SEIZED, SEARCHED, EXAMINED AND HELD IS DESCRIBED AS:

1. Any and all computers, computer program, computer data and/or computer network information as those terms are defined in Penal Law 156.00.
2. Any computers, central processing units, external and internal drives, storage units or media, terminals and video display units, together with peripheral equipment such as keyboards, printers, modems, scanners, or digital cameras and their internal and external storage media.
3. Any and all computing or data processing software, or data including, but not limited to hard disks, floppy disks, magnetic tapes, and integral RAM or ROM units which may reveal evidence which substantiates violations of the aforementioned NY State Penal Law Statutes.
4. The following records and documents, whether contained or stored on the computer, cell phone, magnetic tape, cassette, CD disk, diskette, photo-optical device, Cloud Storage, or any other storage medium, in the form of internet history, SMS, MMS, IM:
 - a. Any access numbers, passcodes, swipe code patterns, passwords, personal identification numbers (PINS), logs, notes, memoranda and correspondence relating to computer, electronic and voice mail systems, Internet addresses and/or related contacts.
 - b. Any computing or data processing literature, including, but not limited to printed copy, instruction books, notes, papers, or listed computer programs, in whole or in part.
 - c. Any audio or video cassette tape recordings, books, magazines, periodicals, or other recorded or printed material, the possession of which constitutes or supports evidence of a violation of Articles 130, 260, and or 263 of the Penal Law of the State of New York.
 - d. Any and all photographs depicting sexual conduct by a child and/or minors engaged in sexually explicit conduct.
 - e. Any records or correspondence relating to the possession, transmission, collection, trading, or production of the aforementioned photographs and/or videos.

5. Any Internet capable device, such as cell phone, tablet, smartphone, gaming system that allows access to the internet and allows for the transmission of data in violation of or supporting a violation of Articles 130, 260, and 263 of the New York State Penal Law.

C. DESIGNATION OR DESCRIPTION OF PLACE, VEHICLE OR PERSON TO BE SEARCHED:

██████████, Fulton NY, located in the Town of Granby, and any other areas the residents may have custody or control of such as, but not limited to, the basement, the garage and other curtilage or vehicles on the property including the blue colored charter bus located on the property.

The residence is located on the north side of Germandale Dr., and is approximately ½ mile west of the intersection of County Road 8. The residence is a white colored mobile home with white skirting. There is a wooden front porch with a wooden railing located in front of the entrance door. The entrance door is white in color and there is dark trim along the roof line, and dark colored shutters on the windows. There is one shutter missing from a front window. To the right of the residence there is a light blue colored charter bus located on the property. There is a gray colored storage shed with white trim located on the right side of the light blue colored charter bus.

D. ALLEGATIONS OF FACT IN SUPPORT OF STATEMENT THAT THERE IS REASONABLE CAUSE TO BELIEVE THAT PROPERTY OF A KIND OR CHARACTER DESCRIBED IN SECTION 690.10 OF THE CRIMINAL PROCEDURE LAW MAY BE FOUND IN OR UPON A DESIGNATED OR DESCRIBED PLACE, VEHICLE OR PERSON:

I am the applicant herein and am a public servant of the kind specified in Section 690.05, Subdivision 1 of the Criminal Procedure Law, my title being that of Investigator with the Division of New York State Police. I am currently assigned to the New York State Police Computer Crime Unit – Central Region. I have been a sworn police officer in NY since January 7, 2002, and member of the New York State Police since April 7, 2003. Your affiant has attended various training classes as it pertains to death investigations, assaults, sex offenses, and drug and narcotic investigations. As part of my tenure as a police officer your affiant has attended numerous state and local training workshops and seminars, on a wide variety of investigations as described above. Your affiant has also received training at the New York State Police Academy. While employed as a police officer your affiant has gained experience by conducting traditional police investigations/operations, and executed or assisted with the execution of search warrants which have resulted in the arrest and or conviction of those responsible. I have been involved in the investigation of offenses relating to computers and the Internet, as well as investigations involving the distribution of child pornography via the Internet. I have received training on the subject of online criminal investigation, the distribution, trading and downloading/sharing of child pornography, and computer evidence handling and forensics. I have received training in Internet investigative techniques as they apply to child pornography investigations. Investigators with the Internet Crimes Against Children Task Force have instructed me in techniques of child pornography investigations. Additionally I have received training in cyber investigations and identifying and seizing electronic media, as well as ways that suspects utilize computers and other electronic media to commit crimes, store evidence of those crimes and conceal evidence of the crimes. I have a Bachelor's degree in Cybersecurity and Information Assurance with a concentration in cybercrime investigations and forensics from Utica College, a Graduate Certificate in Computer Forensics from the University of Central Florida, and a Master's degree in Telecommunications and Network Management from Syracuse University.

Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish reasonable cause to believe that evidence of violations of New York State Penal Law Sections 130, 260, and 263 will be located within the above-described premises.

E. DEFINITIONS

The following non-exhaustive list of definitions applies to this affidavit:

- "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries.
- "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct.
- "Cloud Computing" refers to the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The "Cloud" allows data in the form of documents, pictures, videos, music and any other medium to be uploaded to an account on a service provider's server and accessed by users utilizing various methods such as computers, tablets, smart phones, etc. It is an off-site storage medium for items typically stored/saved on a computer.
- "Cloud Storage" Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network (typically the Internet).
- "Computer" as used herein, is defined in article 156.00 of the Penal Law, as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
- "Computer hardware" as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, USB flash drives, and diskettes, and other memory storage devices); mobile telephone devices, portable memory devices, portable electronic music players, video gaming systems; peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks) and wireless devices, capable of connecting other computer hardware to the Internet.
- "Computer passwords and data security devices" as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- "Encrypt" is the process of converting data into a code preventing unauthorized access. It is the process of hiding and or preventing access to the data by unauthorized users, or users who do not have the credentials to access such data.
- "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
- "Image" or "copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

- "NCMEC" refers to The National Center for Missing and Exploited Children (NCMEC), which serves as a centralized cyber tip line as it pertains to exploited and missing children. Electronic service providers (ie: Google, Microsoft, Yahoo, AOL, et. Al.) are mandated to report instances of apparent child pornography and/or child exploitation.
- "Sexual Conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons.

F. CHILD PORNOGRAPHY AND THE INTERNET

I am aware that computers and computer technology have revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of online child exploitation. For instance:

- Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, cellular phones and tablets, directly from digital cameras or using the "Cloud".
- Modems allow computers to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.
- The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. As explained further below, the storage capacity of electronic media used in home computers has increased tremendously within the last several years. These drives can store very large numbers of visual digital image and video files at very high resolution.
- The Internet, the World Wide Web, and other Internet components afford individuals many different, relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.
- Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing email and instant messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most cases.
- As with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained for very long periods until overwritten by other data.
- The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution and possession of child pornography.
- Data that exists on a computer is particularly resilient to complete deletion. Computer files or remnants of such files can be recovered months or even years after they have been stored on a hard drive, deleted, or viewed via the Internet or from external media, such as CDs, DVDs or external hard drives. Electronic files stored on a hard drive can be retained for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using forensic software. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear.

The Operating System marks the file entry as deleted in its list of all of the files on the storage media. Even the entry that has been marked for deletion, remains until the space is needed for a new entry. The data that was associated with that File Name remains on the hard drive until the space is needed and it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space (space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space) for long periods before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve content of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

G. COMPUTERS AND THE EVIDENCE ASSESSMENT PROCESS IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION CASES

This warrant seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for cellular telephones and also for evidence that establishes how computers and cellular telephones were used, the purpose of their use, and who used them. Additionally, the warrant seeks information about the possible location of other evidence.

- This application seeks permission to search and seize records that might be found on computers, cellular telephones and peripheral devices, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive; another form is other electronic media, such as external hard drives. Some of these electronic records might take the form of files, documents, and other data that is user generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.
- Although some records called for by this warrant might be found in user generated documents (such as word processor, picture, and movie files), computer hard drives can contain other forms of electronic evidence that are not user generated. In particular, a computer hard drive may contain records of how a computer has been used, the purposes for which it was used, and who has used these records. For instance, I have learned from computer forensic experts that:
 1. Data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file, or when a particular DVD disc was viewed using Windows Media Player, etc.).
 2. Virtual memory paging systems can leave traces of information on the hard drive that show what tasks and processes on the computer were recently in use.
 3. Web browsers, email programs, and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords. It can also provide information about who was using the computer, and when they were using the computer.
 4. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use.
 5. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information may be evidence of a crime, show the existence and location of evidence in other locations on the hard drive, and may provide information about the user of the computer.
 6. Further, in finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, I know that when a computer has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created. For example, by reviewing the Internet Browser History, such as Index.dat files (a system file that keeps track of historical activity conducted in the Internet Explorer application), Link (.lnk) files, and thumbs.db

I. Overview of the Current Investigation:

On January 15, 2016 William B. Raymond provided a supporting deposition indicating evidence of the aforementioned crimes may be located at [REDACTED] in the Town of Granby. William Raymond observed images and videos of child pornography while residing at this residence during August through September of 2015. An account of these events is included in the attached supporting deposition. It is alleged by William B. Raymond that his uncle Clif had sexually abused a child and that Clif Seaway possessed photographs he had taken of a young girl who had stayed overnight at his residence several years ago. The deposition is attached for further details.

On January 19, 2016, an inquiry with the Integrated Justice Portal provided information from the New York State Department of Criminal Justice Services that Clif John Seaway Date of birth [REDACTED] 1956 was arrested by Watertown City Police Department on February 13, 2009 for PL 260.10 Sub01, Act in manner to injure child less than 17.

On January 19, 2016 I contacted the City of Watertown Police Department and spoke to Detective Steve Backus to inquire about further details of the arrest indicated on Clif Seaway's criminal history. Detective Backus advised there was no information in their system for an arrest related to an incident on the date of February 13, 2009. Detective Backus further advised Clif Seaway date of birth [REDACTED] 56 was the suspect in a sexual abuse 1st investigation in 2005. An 8 year old female alleged that on or about Sunday September 25, 2005. Clif Seaway had touched the child in her "pee-pee" area and Clif Seaway had the victim touch his penis. The investigation was reported to be closed due to the witness being unavailable for grand jury testimony and negative results in attempting to make contact with the victim and her mother.

On February 17, 2016 an inquiry through the NY Integrated Justice Portal verified the address on file with the NY Department of Motor Vehicles for Clif J. Seaway with the date of birth 05/[REDACTED]/56 is [REDACTED] G. [REDACTED], Fulton, NY 13069.

J. CONCLUSION AND SPECIFIC REQUEST

Based upon the investigation your Affiant has conducted and the information provided to your Affiant by William B Raymond, your Affiant has cause to believe that a computer or computers located at 118 Germandale Drive in the Town of Granby may contain images of child pornography, and has made these images of child pornography available for distribution via the Internet, in violation of Article 130, 260, and 263 of the Penal Law. Your Affiant further states that there is reason to believe that evidence will be found at 118 Germandale Drive in the Town of Granby that constitutes evidence of this crime. Based upon the training I have received, as well as experience conducting child pornography investigations that have led to the execution of search warrants and subsequent examinations of computer systems, I have learned that people who buy, produce, trade or sell child pornography rarely, if ever, dispose of their sexually explicit materials, and they treat these materials as "prized possessions." In addition, based upon my experience in the field of computer crime investigations, I know that information, including images, can easily exist on a computer for days, months, even years after it is "deleted" by the user. This information can be extracted from the computer during a forensic examination of the system.

I further know that conducting a search of a computer system, documenting the search and making an image or evidential copy is a lengthy process. It is necessary to determine that no security devices are in place that could cause the destruction of evidence during the search. In some cases, it is impossible to even conduct the search without expert assistance. Since computer evidence is extremely vulnerable to tampering or destruction, examination will require removal of the system from its present location and transferal to our

(Windows XP) or thumb cache (Windows 8 and 10) files, the forensic examiner can often determine whether a user actually accessed, or attempted to access, images/videos, and whether that user accessed other information close in time to the file creation dates, times and sequences to establish user identity and exclude others from computer usage during times related to the criminal activity.

7. Evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device and requires analysis of the digital device as a whole to demonstrate the absence of particular data. Evidence of the absence of particular data on a digital device cannot be segregated from the digital device.
8. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user, and contextual evidence excluding a computer user. These types of evidence may show ownership, knowledge, and intent. It also may be exculpatory evidence, which I would be required to turn over to the defense in the event charges were brought.
9. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in this affidavit falls within the scope of the warrant.

H. Characteristics of Collectors of Child Pornography:

Consistent with these search results, based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and receive and/or advertise images of child pornography, including:

- The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
- The majority of individuals who collect child pornography collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless enable their sexual fantasies involving children.
- The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, torrents, e-mail, bulletin boards, internet relay chat, newsgroups, instant messaging, and other similar vehicles.
- The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.
- The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.
- The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage.

Forensic Computer Lab at Division Headquarters in Albany or their designee, which will assist in retrieving the records and data authorized to be seized in a controlled environment.

Your Affiant recognizes that some of the above-described property is data that will be contained on said computer in electronic and machine-readable media, which is not readable, by your deponent in its present state. By this application your Affiant requests authorization for himself and other searching members to seize, examine, listen to, read, view and maintain the above-described property and to convert it to humanly readable and viewable form as necessary.

Wherefore, I respectfully request that the Court issue a search warrant and order of seizure of the aforementioned described property located at ~~100 Commando Drive~~ ~~100 Commando Drive~~, NY, in the Town of Granby in order that it may be ascertained if any such property constitutes, substantiates or supports the violations of Articles 130, 260, and 263 of the Penal Law of the State of New York. Additionally, it is requested that any and all seized property of the aforementioned described manner be held for analysis and evaluation at the New York State Police Computer Crime Unit Forensic Laboratory in Albany, NY or their designee.

It is further requested that such warrant authorize the executing police officer to enter the premises to be searched without giving notice of his authority or purpose based upon the fact that computer material can readily be destroyed, or encrypted, almost instantly if it is not secured immediately upon arrival at the premises.

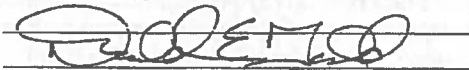


Signature

~~Investigator Michael R. Eckler~~
(Investigator Michael R. Eckler)

Subscribed and sworn to before me

This 18th day of February 2016.



Hon. Donald E. Todd

County Court Judge
Sitting as a local
criminal court pursuant
to CPL 10.20(3)

SUPPORTING DEPOSITION (CPL § 100.20)

THE PEOPLE OF THE STATE OF NEW YORK
VS

CLIF SEAWAY
DEFENDANT(S)

LOCATION OF INCIDENT:

STATE OF NEW YORK, LOCAL CRIMINAL COURT
COUNTY OF OSWEGO
TOWN OF GRANBY

LOCATION OF DEPOSITION:

STATE OF NEW YORK
COUNTY OF ONONDAGA
City OF Syracuse

DATE:

1-14-16

TIME STARTED

11:30

☒ AM☐ PM

FULL NAME:

WILLIAM RAYMOND III

On

at

I,

residing at

555 south state street, Syracuse, NY

with contact information

PHONE NUMBER

STATE THE FOLLOWING:

I am speaking with Inv. Miller at the Onondaga County Justice Center. I would like to give him information about my Uncle Clif Seaway who lives at ~~444 Onondaga Drive~~ in the Town of Granby. I used to live there with him from August of 2015 through September 20, 2015. While I lived there with him, he and I worked on computers together, repairing and rebuilding them for other people. I had a girlfriend at the time who was 13 years old. She is the reason that I am locked up here at the jail. I saved some information on Clif's computer off my microSD card from my phone because I was letting my cousin use my microSD card. I started showing my Uncle Clif some pictures that I had on my phone of old girlfriends. I was showing him from his computer because I had saved my files onto his computer. After I showed him some pictures of girls, he said that he has some pictures. His exact words were "Give me an age?" I told him that I didn't care that I liked it all, not realizing what he had on his computer. Clif then showed me pictures of naked female kids that were under 10 years old. I know they were less than 10 years old because I have 7 kids between the ages of 5 and 16. The pictures of the kids were nude and posing in sexual ways. For example, there was a picture of a young girl about 6 years old sitting in a spread eagle position. Another picture I remember was an underage girl on her hands and knees in a doggy style pose and the picture showed her vagina from the back, and she was looking back at the camera. He has a folder on one of his hard drives that he plugs into his main computer tower. This hard drive is in a bronze or gold outer cover. He keeps this folder with his pictures as a hidden folder. He also showed me videos from this folder also. These videos that I saw were of young girls less than 10. One of the videos that I specifically remember was a naked girl approximately 5 or 6 years old laying on a bed. An adult female was rubbing her naked chest and bare vagina in the video, and you could tell that an adult male was filming it because you could see his legs that appeared as an adult male's legs. Another video I remember was of a naked girl around 11 or 12 dancing. She was rubbing herself in a way that appeared as if she was masturbating. I would say that there are at least 100 images and videos on his computer. One time when I was working on an old IBM server at his house, my Uncle Clif asked me to see if there was a DVD hidden inside the server. I told him that I couldn't find the disk for him and then he ended up telling me that the disc was one that he made. He told me that one of his daughter's friends had come over to spend the night when they lived in Indian Hill trailer park. This would have been about 5 or 6 years ago, and his daughter, would have been around 7 or 8. He said that his daughter's friend brought over some lacey lingerie to sleep in so he thought someone was abusing her. He told me that he took a video and pictures of her at his trailer. He also told me that he was playing with her, but he was not specific about it and I walked out of the room. When I couldn't find the DVD, my Uncle Clif told me that it was probably out in the bus. He has an old International school bus out behind his trailer. It is painted light blue and he has all sorts of things stored out there.

Exhibit D

GENL-4 (04/08)

New York State Police

SUPPORTING DEPOSITION (CPL § 100.20)

Page 2 of 2

THE PEOPLE OF THE STATE OF NEW YORK

VS.

Clif Seaway
DEFENDANT(S)

He told me that he had bondage items stored out on the bus as well. My Uncle has issues with young kids because I've heard him say that these young kids are made to do these things when he was talking about his videos. I asked him what that meant and he said that they are raised this way. My Uncle also plays this virtual game called "Second Life" and he plays this game as a 5 year old girl. I asked him why he plays as a 5 year old and he told me that he has never grown up. He attaches images of naked kids to his room within this game and allows people to come into his room and view them. I know this because I have watched him play this game on the same computer that he has the child pornography. I have used my Uncle's computer when I lived there as well. I know my Uncle's password for his computer, which is lowercase "seadj123." The only thing I have ever put on my Uncle's computer was the files from my MicroSD card from my cell phone. I put them in a folder that I labeled "Billy's phone."

NOTICE

(Penal Law Sec. 210.45)

In a written instrument, any person who knowingly makes a false statement which such person does not believe to be true has committed a crime under the laws of the state of New York punishable as a Class A Misdemeanor.

Affirmed under penalty of perjury

this 14th day of January, 20 16

- or -

*Subscribed and Sworn to before me

this _____ day of _____, 20 _____

(SIGNATURE OF DEPONENT) - Error Reference source not found.

(WITNESS)

TNV BMM II

(NAME OF PERSON TAKING DEPOSITION)

TIME ENDED
1:05☐ AM
☒ PM

*This form need be sworn to only when specifically required by the court.

Exhibit D

GENL-19 REV (04/08) VOLUNTARY STATEMENT

NEW YORK STATE POLICE

VOLUNTARY STATEMENTCOUNTY OF OSWEGO
TOWN OF VOLNEYSTATEMENT START TIME: 12:43 ☐ AM ☒ PM
DATED: FEBRUARY 24, 2016

I, CLIF J. SEAWAY, AGE: 59 AND BORN ON: 7/27/56, AND RESIDING AT: 1 [REDACTED] DRIVE IN THE TOWN OF GRANBY, HAVE BEEN ADVISED BY: INV. BENJAMIN MILLER, OF THE NEW YORK STATE POLICE, OF THE FOLLOWING:

☒ CS I HAVE THE RIGHT TO REMAIN SILENT AND I DO NOT HAVE TO MAKE ANY STATEMENT IF I DO NOT WANT TO.

☒ CS IF I GIVE UP THAT RIGHT, ANYTHING I DO SAY CAN AND WILL BE USED AGAINST ME IN A COURT OF LAW.

☒ CS I HAVE THE RIGHT TO HAVE A LAWYER PRESENT BEFORE MAKING ANY STATEMENT OR AT ANY TIME DURING THIS STATEMENT.

☒ CS IF I SHOULD DECIDE THAT I DO WANT A LAWYER AND CANNOT AFFORD TO HIRE ONE, A LAWYER WILL BE APPOINTED FOR ME FREE OF CHARGE AND I MAY HAVE THAT LAWYER PRESENT BEFORE MAKING ANY STATEMENT.

☒ CS I ALSO UNDERSTAND THAT I HAVE THE RIGHT TO STOP AT ANY TIME DURING THIS STATEMENT AND REMAIN SILENT AND HAVE A LAWYER PRESENT.

I FULLY UNDERSTAND THESE RIGHTS AND AT THIS TIME, I AGREE TO GIVE UP MY RIGHTS AND MAKE THE FOLLOWING STATEMENT;

Inv. BM Miller
WITNESS

☒ CS Clif J. Seaway
CLIF J. SEAWAY

☒ CS I am speaking with Inv. Benjamin Miller of the New York State Police, and Special Agent Lon Ziankoski of Homeland Security Investigations at the New York State Police in Fulton. The police came to my house today with a search warrant and they told me they were there to look through the house. I told them that I thought that I knew why they were there. I showed the police two VHS tapes that were in the rear bedroom. These were tapes that came out of a cabinet that my nephew, Billy Raymond, had taken from me, and put them in the back room. I have never watched these tapes, but, I suspect that there may be video of an underage girl on them. I only suspect this because I had cameras set up in my house, and Billy took them down and brought them to the back bedroom. I believe Billy could have had sex with her in my house in that bedroom, and he could have taped it with those cameras. I don't know this for sure, but I know one of the charges that Billy is in jail for, is for having sex with this underage girl. I found out later that this girl was 13 years old, but, at the time she was with Billy in my

☒ CS